Application Number	: 10/803,167	Confirmation Number: 4158
Applicant	: Robert N. Nazzal	
Filed	: 16 March 2004	
T.C./A.U.	: 2436	
Examiner	: Colin, Carl G.	
Docket Number	: RIV-0580	
Customer No.	: 22835	

Interview Summary
Via electronic filing

INTERVIEW SUMMARY

Dear Examiner Colin:

In light of the interview on **11 May 2009**, please find an interview summary below.

Identification of Claims and Reference Discussed

Claim(s) for discussion: 1 and 8

Reference(s) for discussion: Porras et al. (U.S. Pub. No. 2004/0010718, hereinafter "Porras"), Pruthi et al. (U.S. Patent No. 7,492,720, hereinafter "Pruthi"), and Cooper et al. (U.S. Patent No. 7,047,288, hereinafter "Cooper").

Applicant's Arguments

With respect to claim 8, Applicant submits that the new service alert rule in the present system is specific to whether a host is **providing** or **using** a new service. The main reference used in the Office Action, Porras, does not distinguish between hosts that a **providing** a new service and hosts that are **using or consuming** the new service.

With respect to claim 1, Applicant has redrafted the claim to more clearly represent the UI depicted in FIG. 10 of the instant application. Applicant will explain the functions of each field of this UI in more details during the phone call.

Proposed Amendment:

1. (Currently amended) A graphical user interface rendered on a display device ~~the graphical user interface~~ for configuring a new service ~~detection process~~alert rule, the graphical user interface comprising:

a first field that ~~depicts choices for entities~~allows a user to specify an entity to track in the network;

a second field that allows the user to specify ~~a system to track if the selected entity is providing or consuming a service~~whether the rule is to be applied when the specified entity is providing or consuming a new service;

a third field that ~~depicts a range over which to track an entity selected in the first field~~allows the user to specify a range of network entities to which the new service is unprecedented; and

a fourth field that allows the user to specify a severity for an alert generated if a new service is detected.

8. (Currently amended) A method for detection of a new service involving host in a network, the method comprises:

retrieving a baseline list of port and/or service protocols used by a host being tracked, the baseline list listing service and/or port protocols used by that host over a baseline period that is of a longer duration ~~that~~ than a current period;

retrieving a current list of service and/or port protocols for the current period used by the host being tracked;

determining whether there is a difference in the protocols, by finding a protocol that was in the current list but was not in the baseline list; and if there is a difference;

determining whether the host is providing or using the new service;

identifying an alert rule corresponding to whether the host is providing or using the new service; and

issuing an alert based at least on the identified alert rule~~indicating a new service involving the tracked host.~~

Interview Summary

Examiner suggested clarifying claim 1 so that it recites a system with a display device. Examiner suggested clarifying that the alert is issued based on whether the service is provided or used as specified in the user's input in the second field.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 13 July 2009

Shun Yao
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com